

Sphinx Feature List

Sphinx Versions

The Sphinx software is available in three versions, to meet the needs of all types and sizes of organizations.

The list below indicates the features that are included in each Sphinx version. See also www.odsphinx.com for additional information.

Version	Order #	Description	Included software components
Sphinx Standalone	S-20	No management or issuance system required. <ul style="list-style-type: none"> • Install Sphinx Logon Manager software and desktop card readers on end-user computers. • End-users present their IDs card to card readers to self-enroll with Sphinx, and start protecting their logon data. 	Sphinx Logon Manager, for end-user computers
Sphinx Enterprise	S-30	Easy setup and self-enrollment features of Sphinx Standalone version, plus: <ul style="list-style-type: none"> • Pre-configured Sphinx CardMaker management software, runs "out-of-the-box" on administrator server computer. • Administrators who want more control can change the default settings of this full-featured software to specify PIN and password policies, link to HR databases, and much more. 	Sphinx Logon Manager, for end-user computers Sphinx CardMaker, for administrator computer
Sphinx Enterprise PKI	S-30-PKI	All functionality of Sphinx Enterprise version plus: <ul style="list-style-type: none"> • PKI card interface and "middleware" is built-in, enabling the ID card to support the full spectrum of certificate-based functions, such as email encryption and digital signatures for documents. 	Sphinx Logon Manager, for end-user computers Sphinx CardMaker, for administrator computer PKI middleware, for all computers

Windows Logon Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Card-secured logon to Windows	<p>End-user presents card to card reader and enters card PIN to logon to Windows. Sphinx transfers logon data to Windows logon process transparently so that keystrokes cannot be observed or recorded.</p> <p>Standard Sphinx installations use Microsoft GINA-based logon to Windows. Sphinx Logon Manager software reads user name, password, domain from card (or card server for proximity cards) and passes this data to the Windows logon process on the end-user's computer, via the Microsoft GINA API. Does not replace or change Microsoft GINA; only interacts with relevant functions.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Settings Menu > Logon to Windows. CardMaker Administrator's Manual: Configuration > Card Settings > Logon to Windows.</i></p>	✓	✓	✓
PKI certificate-based logon to Windows	<p>When Sphinx is used with a Public Key Infrastructure (PKI), the Sphinx PKI middleware provides standard CSP and PKCS#11 card interfaces, which enables the card to be used for certificate-based functions.</p> <p>End-user presents card to card reader and enters card PIN to logon to Windows. The Microsoft logon process uses the Kerberos v5 with PKINIT authentication protocol for domain and local access. The Microsoft GINA has built-in support for this functionality for Windows 2000 or higher. See also PKI Features.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Getting Started > PKI Usage Notes.</i></p>			✓

Sphinx Feature List

End-user managed Windows logon data	<p>By default, upon first use, cardholder is prompted to enter his existing Windows logon data into Sphinx Logon Manager. With next system reboot, cardholder is prompted to present card and enter PIN to logon to Windows.</p> <p>Note: Logon data which end-user saves with Sphinx cannot be accessed by Administrator.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Settings Menu > Logon to Windows.</i></p>	✓	✓	✓
Administrator managed Windows logon data	<p>Administrator may choose to preset Windows logon entry data for individuals or groups of cards. Administrator can also continue to manage Windows logon data for cardholders if desired, by updating Windows logon data in cardholder account.</p> <p>For entries created by Administrator, Administrator can specify if end-user will be allowed to view or change the logon data. See also Managed Entry Features.</p> <p>In order to use this feature, card data must be stored on the CardMaker server. This feature is not available for smart cards that store data on the card, but smart card installations can opt to load preset Wizard entries to cards at issuance. See also Logon Entries Wizard, below.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Tools > Managed Entries, and Appendix: Using Sphinx With Active Directory.</i></p>		✓	✓
Synchronized Active Directory enrollment for Windows logon	<p>When this option is activated, Sphinx automatically enrolls new end-users in Active Directory and updates the accounts of existing users upon card issuance. Once the end-users have the cards in their hands, all cards can immediately be used to logon to network computers.</p> <p>Sphinx works with Active Directory to use the Cardholder ID that Administrator enters into Sphinx as the Windows "user logon name". For users who are already known to Active Directory, Sphinx simply resets the Windows password in Active Directory before loading the logon data to the card account. For new users, Sphinx causes a new Active Directory account to be created for the user before generating a new Windows password and loading the data to the card account.</p> <p>Administrator can specify if end-user will be allowed to view or change the logon data.</p> <p>In order to use this feature, card data must be stored on the CardMaker server. This feature is not available for smart cards that store data on the card.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Appendix: Using Sphinx With Active Directory.</i></p>		✓	✓
Logon Entries Wizard	<p>Administrator can pre-enter logon entries for additional Windows logons into cards or card accounts, and the Sphinx Logon Entries Wizard will prompt the cardholder to personalize the entry with their user name and/or password when they open the Sphinx Logon Manager software.</p> <p>For smart cards that store data on the card, Wizard entries can be automatically loaded to the cards of all members of a user group upon card issuance.</p> <p>For card data that is stored on the CardMaker server (ie, RFID cards), Wizard entries can be loaded to card accounts at any time.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Tools > Logon Entries Wizard.</i></p>		✓	✓

Sphinx Feature List

Storage of multiple Windows logons	<p>For end-users with multiple Windows logon identities or domains, Sphinx allows entry and selection of multiple logons.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Settings Menu > Logon to Windows.</i></p>	✓	✓	✓
Pull card to lock, logoff, or shutdown computer	<p>End-user can remove card from reader to lock, logoff, or shutdown workstation. Removal of card invokes the appropriate Windows process.</p> <p>Setting can be established by end-user in Sphinx Logon Manager software or by Administrator in Sphinx CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.</p> <p>In addition to card-removal behavior, workstation can also be locked using an optional sonar device that detects when end-user steps away from workstation. Sphinx is also compatible with this device.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Settings Menu > Logon to Windows. CardMaker Administrator's Manual: Configuration > Card Settings > Windows Logon.</i></p>	✓	✓	✓
Pull card to lock, logoff, disconnect, from Terminal Services session	<p>End-user can remove card from reader to lock, logoff, disconnect, or shutdown from a Terminal Services session. Removal of card invokes the appropriate Windows process.</p> <p>Setting is established by Administrator in Sphinx CardMaker software. Administrator can specify if end-user will be allowed to change this setting.</p> <p>Administrator also has the option to specify that a custom script will be launched upon card removal, also triggering a disconnect of the remote session if desired.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > Windows Logon.</i></p>		✓	✓
Tap in / tap out behavior	<p>Typically used for contactless cards. When this option is activated, the "pull card" action that was specified (as described above) will be triggered upon tapping the card on the card reader.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > Windows Logon.</i></p>		✓	✓
Control Windows "secure screen saver" and "lock workstation" functions from Sphinx	<p>End-user can "lock" Windows session before stepping away from their desk using Sphinx short-cut button. End-user can "unlock" a Windows session that has been locked by Windows "secure screen saver" or "lock computer" functions by presenting card and entering card PIN.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Settings Menu > Logon to Windows.</i></p>	✓	✓	✓
Windows password change synchronization	<p>When end-user changes Windows password in the Sphinx program, password change will be synchronized with Windows so that end-user does not need to enter the change twice. Likewise, if Windows informs end-user at start-up that their password has expired and end-user changes password as prompted, password change will be synchronized with Sphinx program.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Settings Menu > Logon to Windows.</i></p>	✓	✓	✓
Windows password policy control	<p>Administrator can specify required Windows password length and character type (numeric, upper case, lower case...) in Sphinx CardMaker software. and end-user must conform to these</p>		✓	✓

Sphinx Feature List

	<p>requirements when entering or changing Windows password.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > Windows Password Policy.</i></p>			
Generate random Windows password	<p>When end-user changes Windows password, he can generate a random password that conforms to the installation's Windows Password Policy, if applicable. If installation has no Windows Password Policy, end-user can specify password length and character type (numeric, upper case, lower case...) for random password.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Settings Menu > Logon to Windows.</i></p>	✓	✓	✓
Password change reminder	<p>Sphinx can prompt cardholder to change Windows password every specified number of days.</p> <p>Setting can be established by end-user in Sphinx Logon Manager software or by Administrator in Sphinx CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Settings Menu > Logon to Windows. CardMaker Administrator's Manual: Configuration > Card Settings > Windows Password Policy.</i></p>	✓	✓	✓
Password repetition control	<p>Sphinx can prohibit the entry of up to four previously used Windows passwords, when cardholder changes Windows password.</p> <p>Administrator can establish setting in Sphinx CardMaker software.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > Windows Password Policy.</i></p>		✓	✓
System logging of cardholder logon and logoff	<p>When the CardMaker server is active, the system will log when end-users logon to Windows and logoff of Windows with their card. This record can be viewed as a CardMaker transaction report.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Reports > Transactions.</i></p>		✓	✓

Website and Application Logon Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Card-secured logon to websites and applications	<p>End-user presents card to card reader and enters card PIN to logon to websites and applications. Sphinx transfers logon data to logon process transparently so that keystrokes cannot be observed or recorded.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Logon Entries Screen.</i></p>	✓	✓	✓
End-user managed logon entries	<p>By default, cardholder is prompted to auto-record their logon data for websites and save it to their Sphinx account. Application logon data is easily recorded using the Record button. The next time cardholder goes to a website or application that Sphinx knows, cardholder is prompted to present card and enter PIN to logon to website or application.</p> <p>Note: Logon data which end-user saves with Sphinx cannot be accessed by Administrator.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Logon Entries Screen.</i></p>	✓	✓	✓

Sphinx Feature List

Administrator managed logon entries	<p>Administrator may choose to preset logon entry data and load it to end-user Sphinx accounts. Administrator can also continue to manage logon data for cardholders if desired, by updating logon data in cardholder account.</p> <p>For entries created by Administrator, Administrator can specify if end-user will be allowed to view or change the logon data. See also Managed Entry Features.</p> <p>In order to use this feature, card data must be stored on the CardMaker server. This feature is not available for smart cards that store data on the card, but smart card installations can opt to load preset Wizard entries to cards at issuance. See also Logon Entries Wizard below.</p> <p><u>More info:</u> CardMaker Administrator's Manual: Tools > Managed Entries.</p>		✓	✓
Logon Entries Wizard	<p>Administrator can pre-enter logon entries into cards or card accounts, and the Sphinx Logon Entries Wizard will prompt the cardholder to personalize the entry with their user name and/or password when they open the Sphinx Logon Manager software.</p> <p>For smart cards that store data on the card, Wizard entries can be automatically loaded to the cards of all members of a user group upon card issuance.</p> <p>For card data that is stored on the CardMaker server (ie, RFID cards), Wizard entries can be loaded to card accounts at any time.</p> <p><u>More info:</u> CardMaker Administrator's Manual: Tools > Logon Entries Wizard.</p>		✓	✓
Auto-record and auto-fill of logon data	<p>Whenever cardholder enters logon information into a website that Sphinx recognizes as being recordable, Sphinx asks cardholder if he wants to record the logon data. Whenever cardholder goes to a website or application logon location which Sphinx has recorded, Sphinx prompts cardholder to present card and enter PIN, then automatically enters logon data and cardholder is logged on.</p> <p><u>More info:</u> Logon Manager User's Manual: Logon Entries Screen.</p>	✓	✓	✓
Initiate recording of logon data	<p>It's easy to record application logon data using the Record button. Or, end-users who don't want to use the auto-record feature for website logons can switch off this default setting, and click on the Record button to initiate the recording of logon data. The Record button is also useful for websites that don't adhere to typical logon procedures, that Sphinx doesn't recognize as being recordable. In any case, whenever cardholder goes to a logon location which Sphinx has recorded, Sphinx prompts cardholder to present card and enter PIN, then automatically enters logon data and cardholder is logged on.</p> <p><u>More info:</u> Logon Manager User's Manual: Logon Entries Screen.</p>	✓	✓	✓
Manual entry and button-click fill of logon data	<p>For website or application logon locations that don't have a unique address, it's simple for cardholders to create a new logon entry in Sphinx and manually enter logon data. Then to fill logon data, simply open the logon entry in Sphinx and click on the Sphinx "Logon Now" button to transfer logon data to location.</p> <p><u>More info:</u> Logon Manager User's Manual: Logon Entries Screen.</p>	✓	✓	✓
Sphinx pop-up	<p>Whenever cardholder goes to a website or application logon location that Sphinx has stored but which is not designated as auto-fill, Sphinx automatically pops-up with the logon data so that cardholder can complete logon.</p> <p><u>More info:</u> Logon Manager User's Manual: Logon Entries Screen.</p>	✓	✓	✓

Sphinx Feature List

Browse to logon location from Sphinx	End-user can double-click on a website or application entry in Sphinx to browse to that location or start application, and auto-fill or transfer logon data. <u>More info:</u> <i>Logon Manager User's Manual: Logon Entries Screen.</i>	✓	✓	✓
Submit control	Cardholder can choose to submit logon data to logon processes automatically, or can choose to manually control the submission of logon data. With the latter option, cardholder must click on the website or application "Submit" or "Enter" button, to submit logon data. Manually controlled submission of logon data is the default for auto-filled entries. <u>More info:</u> <i>Logon Manager User's Manual: Logon Entries Screen.</i>	✓	✓	✓
"Drag and drop" transferal of logon data	Logon data fields can be "dragged and dropped" into logon entry fields as desired. <u>More info:</u> <i>Logon Manager User's Manual: Logon Entries Screen.</i>	✓	✓	✓
Password policy control	Administrator can specify required password length and character type (numeric, upper case, lower case...) for websites/applications in Sphinx CardMaker software, and end-user must conform to these requirements when entering or changing passwords. <u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > Website/Application Password Policy.</i>		✓	✓
Generate random password	When end-user creates or changes a website or application password, he can generate a random password which conforms to the installation's Password Policy, if applicable. If installation has no Password Policy, end-user can specify password length and character type (numeric, upper case, lower case...) for random password. <u>More info:</u> <i>Logon Manager User's Manual: Logon Entries Screen.</i>	✓	✓	✓
Password change reminder	Sphinx can prompt cardholder to change website or application password every specified number of days. Setting can be established by end-user in Sphinx Logon Manager software or Administrator in Sphinx CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting. <u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > Website/Application Password Policy.</i>	✓	✓	✓
Password change verification	Sphinx can prompt cardholder to verify that password has been changed in website or application. This ensures that passwords remain synchronized (since it would not be possible for Sphinx to automatically change a password in a third party website/application logon location that is not linked to Sphinx via an API). Until cardholder verifies that password has been changed in website/application, Sphinx will not accept password change. Setting can be established by end-user in Sphinx Logon Manager software or Administrator in Sphinx CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting. <u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > Website/Application Password Policy.</i>	✓	✓	✓
Password repetition control	Sphinx can prohibit the entry of up to four previously used passwords, when cardholder changes a website or application		✓	✓

Sphinx Feature List

	<p>password.</p> <p>Administrator can establish setting in Sphinx CardMaker software.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > Website/Application Password Policy.</i></p>			
--	---	--	--	--

Other End-user Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Storage of address and payment information	<p>End-user stores address and payment information in Sphinx, for use in website and application entry fields. The labels of all address and payment entry fields can be customized by the end-user.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Address Entries Screen, and Payment Screen.</i></p>	✓	✓	✓
"Drag and drop" transfer of address and payment information	<p>Cardholder can "drag" address and payment information and "drop" it into website and application entry fields, so that this basic information does not have to be continually re-typed.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Address Entries Screen, and Payment Screen.</i></p>	✓	✓	✓
Backup and restore data	<p>Cardholder can back up all of his Sphinx data to his computer's hard drive, the network, or a removable data carrier such as a memory stick or floppy disk. Sphinx prompts cardholder to enter a backup password. Then, if he loses his contact chip card or forgets the authentication data for his contactless card, he can restore his Sphinx data to a new card as long as he knows his backup password.</p> <p>Setting of backup location can be established by end-user in Sphinx Logon Manager software or Administrator in Sphinx CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Utilities Menu > Backup/Restore. CardMaker Administrator's Manual: Configuration > Card Settings > Backup.</i></p>	✓	✓	✓
Auto-backup reminder	<p>Sphinx can prompt cardholder to backup his Sphinx data every specified number of days at a certain time of day, or after data has been saved to Sphinx a specified number of times.</p> <p>Setting can be established by end-user in Sphinx Logon Manager software or Administrator in Sphinx CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Utilities Menu > Backup/Restore. CardMaker Administrator's Manual: Configuration > Card Settings > Backup.</i></p>	✓	✓	✓
Save Sphinx data to laptop	<p>For card installations that use the Sphinx CardMaker server to store Sphinx entries, cardholders have the option to save their Sphinx data to Laptop Mode, so that they can use Sphinx to access this data without a card, card reader or network connection while they travel with their laptop.</p> <p>Administrator also has the option to disable Laptop Mode, or require that a card and card reader is also required in Laptop Mode, and can specify this setting in the Sphinx CardMaker software.</p> <p><u>More info:</u></p>		✓	✓

Sphinx Feature List

	Logon Manager User's Manual: File Menu > Save to Laptop. CardMaker Administrator's Manual: Configuration > Program Settings > Server.			
Access Sphinx data on CardMaker server remotely	For card installations that use the Sphinx CardMaker server to store Sphinx data, this feature enables user to access Sphinx data on server without a card or card reader, when traveling. For security reasons, this option is typically only made available upon user request - for example, if user forgot to load Sphinx data to laptop before leaving headquarters. Administrator can activate this capability on an individual basis for a defined period of time in the Sphinx CardMaker software. <u>More info:</u> CardMaker Administrator's Manual: Configuration > Program Settings > Server.		✓	✓
No training required	End-user interface is intuitive and easy to use. Software prompts guide end-user through program.	✓	✓	✓
Auto-start and minimize	Sphinx Logon Manager software automatically starts at system startup, so that it is available for logons throughout the session. After auto-start, software automatically minimizes to the system tray. Thereafter, Sphinx auto-fills logon data or end-user double-clicks on Sphinx icon to access software, as required. These default setting can also be switched off according to user preference. Administrator can control auto-start capability as desired in the Sphinx CardMaker software. <u>More info:</u> Logon Manager User's Manual: Settings Menu > General. CardMaker Administrator's Manual: Configuration > Card Settings > General.	✓	✓	✓

PKI Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
One step installation of middleware software	PKI middleware software self-installs at end-user and administrator computers and is ready for immediate use, with no additional configuration required. <u>More info:</u> Logon Manager User's Manual: Getting Started > PKI Usage Notes. CardMaker Administrator's Manual: Getting Started > Administrator Software Installation.			✓
Seamlessly integrated with Sphinx	The Sphinx PKI middleware has been fully integrated with the Sphinx software in the Sphinx Enterprise PKI version. End-users can use Sphinx Logon Manager software functionality and PKI functionality seamlessly together using a single card. Administrators manage the solution using the Sphinx CardMaker software interface. Note: Features described under Windows Logon Features refer to GINA-based logon features. Certificate-based Windows logon features that an organization chooses to implement will be independent of the GINA-based logon features. <u>More info:</u> Logon Manager User's Manual: Getting Started > PKI Usage Notes. CardMaker Administrator's Manual: Getting Started > Administrator Software Installation.			✓
Standards based	Includes PKCS#11 library, and Cryptographic Service Provider (CSP) for applications supporting Microsoft CryptoAPI. Supports all major standards and interfaces including PKCS #11. Microsoft			✓

Sphinx Feature List

	CryptoAPI, PC/SC, PKCS #12, PKCS #15.			
Secure storage	On-board cryptographic key generation up to 2,048 bit. Secure storage of X.509 digital certificates. Multiple key and certificate storage.			✓
Seamless Windows compatibility	Fully transparent Windows logon (2000, XP, Vista, 2003). Seamless integration in Windows: secure user authentication, e-mail signing and encryption, VPN, network access, logon, and Terminal Services (Windows 2003).			✓
Supported PKI systems	Baltimore, Entrust, eTrust, Global Sign, Microsoft, RSA, SafeGuard, SafeLayer, Verisign.			✓
Supported applications	VPN: Check Point, Cisco, Microsoft, NCP. Secure e-mail clients: Microsoft Outlook (98, 2000, XP, Vista, Express), Novell Groupwise 6, Mozilla Thunderbird, Mozilla Firefox. SSL authentication for browsers: Microsoft Internet Explorer, Mozilla Firefox. Other applications: Citrix, Lotus Notes, PGP, SSH Tectia Client, RSA SecurID, SafeBoot, Utimaco.			✓
Interoperability	Works out-of-the-box with a diversity of state-of-the-art cards and tokens. See Solution Packages at www.odsphinx.com .			✓

Setup Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Easy installation of end-user software	Pre-configured Sphinx Logon Manager software self-installs at end-user computers and is ready for immediate use, with no additional configuration required. Sphinx Logon Manager setup is based on Microsoft Installer, which is compatible with numerous network installation tools. <u>More info:</u> <i>Logon Manager User's Manual: Getting Started.</i>	✓	✓	✓
Easy installation of administrator software	Pre-configured Sphinx CardMaker software self-installs at administrator server computer. Administrator specifies only three server settings, imports license keys, and software is ready for immediate use, with no additional configuration required. <u>More info:</u> <i>CardMaker Administrator's Manual: Getting Started.</i>		✓	✓
Easy import of license keys	Use the Sphinx CardMaker software to load the license keys to your Sphinx installation, with a couple of mouse clicks. Sphinx license keys are based on the number of cardholders, with a unique license key for each cardholder. <u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Key File.</i>		✓	✓
No change to network or Windows setup	Requires no change to existing network setup or user accounts on domain server. Requires no change to existing Windows setup. Logon to Windows performs according to standard Windows protocols for Standalone as well as networked computers (NT Domain Servers, Active Directory).	✓	✓	✓
No change to RFID card setup	Requires no change to existing configuration of RFID cards that are compatible with Sphinx. Cardholders can self-enroll with Sphinx using the cards they already have, with no administrator involvement. The added logical access functionality with Sphinx does not impact on any other RFID card functions (such as facility	✓	✓	✓

Sphinx Feature List

	access control, time & attendance or e-purse functions). When a Sphinx installation is setup to store data on the card, Sphinx can be pre-configured to only use the available free sectors on the card.			
--	--	--	--	--

Auto-enrollment Features (Standalone installations or installations that store data on the server)

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
No configuration required	Software is pre-configured with standard default settings and ready for end-user self-enrollment immediately after installation. <u>More info:</u> <i>Logon Manager User's Manual: Getting Started > Sphinx Self Enrollment.</i>	✓	✓	✓
End-user self-enrollment	By default upon first use, cardholder presents card to card reader and is prompted to enter Windows user name and password to register with Sphinx server. Administrator can change the default settings, to also require entry of name and employee ID#, as desired. This information (except for Windows password) will populate the CardMaker cardholder database. Cardholders with Sphinx Standalone version will instead be prompted to enter their Sphinx license key. Sphinx software is then ready for immediate use. <u>More info:</u> <i>Logon Manager User's Manual: Getting Started > Sphinx Self Enrollment. CardMaker Administrator's Manual: Card Issuance > Self Enrollment, and Configuration > Program Settings > Server.</i>	✓	✓	✓
End-user self re-enrollment	By default, if end-user loses his card and is given a new card, he can self re-enroll with Sphinx and access his previous Sphinx data if he knows his personal security code. Note: Standalone users must have a backup of their previous Sphinx data and know their backup code, if they want to use previous data with their new card. Administrator can change the default, to disallow self re-enrollment, as desired. <u>More info:</u> <i>CardMaker Administrator's Manual: Card Issuance > Self Enrollment, and Configuration > Program Settings > Server.</i>	✓	✓	✓

Managed Enrollment Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Customizable settings	Installation can use manufacturer's software default settings. Or, Administrator can change software settings in Sphinx CardMaker software before issuing cards, to reflect corporate security policies and control how the end-user uses Sphinx. <u>More info:</u> <i>CardMaker Administrator's Manual: Card Issuance > Issue Cards, and Configuration > Program Settings/Card Settings.</i>		✓	✓
Database importing	Employee data can be imported from HR database into Sphinx CardMaker software before card issuance, if required. Built-in data import functions support ODBC and LDAP compatible databases. Sphinx CardMaker can also be linked with facility access control card management system if desired. <u>More info:</u> <i>CardMaker Administrator's Manual: Tools > Data Import.</i>		✓	✓

Sphinx Feature List

User groups	Administrator can specify different default card settings and managed entries for different user groups, for example, "Sales Department" or "Management". <u>More info:</u> <i>CardMaker Administrator's Manual: Card Issuance > Issue Cards, and Configuration > Card Settings.</i>		✓	✓
One step issuance	Administrator clicks "Issue Card" in Sphinx CardMaker software and chooses end-user from database, or enters end-user data, to issue card. <u>More info:</u> <i>CardMaker Administrator's Manual: Card Issuance > Issue Cards.</i>		✓	✓
ID card printing	Administrator has the option to print ID cards as a part of the issuance step, using a TWAIN compatible webcam and an ID card printer. Allows for full color printing on one side, with photo, name, ID#, and additional fields as desired. <u>More info:</u> <i>CardMaker Administrator's Manual: Card Issuance > Issue Cards.</i>		✓	✓
Lost or stolen card "hotlist"	When a card is lost or stolen, it can be reported to the Sphinx CardMaker software so that it will no longer be accepted within the Sphinx system. <u>More info:</u> <i>CardMaker Administrator's Manual: System Maintenance > Report Lost/Stolen/Defective/Returned Card.</i>		✓	✓
One step card re-issuance	After a card has been hotlisted, a new card can be re-issued to the cardholder by selecting the cardholder's name from the cardholder list. <u>More info:</u> <i>CardMaker Administrator's Manual: System Maintenance > Re-issue Card.</i>		✓	✓
Recycle card	All Sphinx card data can be erased using the Sphinx CardMaker software, so that the card can be re-used and issued to another user. <u>More info:</u> <i>CardMaker Administrator's Manual: System Maintenance > Recycle Card.</i>		✓	✓
Reports	Complete cardholder reports and transaction logs are available in the Sphinx CardMaker software. <u>More info:</u> <i>CardMaker Administrator's Manual: Reports.</i>		✓	✓

Managed Entries Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Easy creation of managed entries	Administrator simply creates a logon entry using the Sphinx Logon Manager software and saves it. When the administrator "auto-records" the logon entry, Sphinx "learns" the logon location of the entry, and the formats for user name, password and other entry fields. <u>More info:</u> <i>CardMaker Administrator's Manual: Tools > Managed Entries.</i>		✓	✓
Easy assignment of managed entries to user groups or individuals	Administrator assigns managed entries to user groups or individuals, and edits user name and password information as required for the group or individual. <u>More info:</u> <i>CardMaker Administrator's Manual: Tools > Managed Entries.</i>		✓	✓

Sphinx Feature List

Simple managed entry screen	Managed entries are easy to edit using the Managed Entries screen in the Sphinx CardMaker software, where Administrator has an overview of all managed entries and can easily select, edit, and assign managed entries. <u>More info:</u> <i>CardMaker Administrator's Manual: Tools > Managed Entries.</i>		✓	✓
End-user edit control	Administrator can specify if user group or individual end-user will be allowed to view, edit all, edit password, or delete the managed entry. <u>More info:</u> <i>CardMaker Administrator's Manual: Tools > Managed Entries.</i>		✓	✓
Storage control	Administrator can specify if the managed entry will be stored on the end-user card and on the server, or stored only on the Sphinx server. <u>More info:</u> <i>CardMaker Administrator's Manual: Tools > Managed Entries.</i>		✓	✓
No additional programming required	Many other logon management systems require that the administrator program links to the applications for which logon entries will be managed. No programming is required with Sphinx. The managed entries functionality works as easily as all of the other Sphinx features. <u>More info:</u> <i>CardMaker Administrator's Manual: Tools > Managed Entries.</i>		✓	✓
API for identity management systems	All managed entries are available via an API for 3rd party identity management and provisioning systems. Interfaces are based on ODBC, LDAP and XMP-RPC standards.		✓	✓

Other Administrator Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Administrator program protection	Administrators logon to Sphinx CardMaker using Administrator password, or based on the administrator rights granted to their card. <u>More info:</u> <i>CardMaker Administrator's Manual: Card Issuance > Administrator Rights.</i>		✓	✓
Administrator assignment	Primary Administrator grants or revokes Sphinx CardMaker rights for other Administrators. <u>More info:</u> <i>CardMaker Administrator's Manual: Card Issuance > Administrator Rights.</i>		✓	✓
Activity log	When Administrators logon to Sphinx CardMaker with their card, the activity log automatically records which administrator performed each activity. <u>More info:</u> <i>CardMaker Administrator's Manual: Reports > Transactions.</i>		✓	✓
Master / slave administrator stations	When more than one administrator workstation is required for card issuance and administration, the Sphinx CardMaker software can be installed on one or more secondary workstations, which can be configured to operate in Slave mode. When operating in Slave mode, the admin station accesses all configuration files on the Master computer and accesses the database files as configured on the Master. <u>More info:</u> <i>CardMaker Administrator's Manual: Getting Started > Master/</i>		✓	✓

Sphinx Feature List

Slave Workstation.

Security Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
User designated PIN	By default upon first use, cardholder is prompted to choose a unique Personal Identification Number (PIN). This PIN, along with presentation of the card, will be required for all access to the Sphinx Logon Manager software. <u>More info:</u> <i>Logon Manager User's Manual: Getting Started > Changing Default Card PIN.</i>	✓	✓	✓
User designated PUK	By default upon first use, cardholder is prompted to choose a unique Personal Unlock Key (PUK). The PUK is a second card PIN, which the cardholder can use to unlock their card. A card will be locked and no longer accepted within the Sphinx system if the cardholder enters the wrong PIN multiple times. Once a card has been locked, Sphinx will prompt the cardholder to enter the PUK to unlock the card. <u>More info:</u> <i>Logon Manager User's Manual: Getting Started > Changing Default Card PIN.</i>	✓	✓	✓
Randomly generated PIN/PUK option	Most Sphinx installations use the standard default initial PIN of "12345", which the end-user is prompted to change upon first use. This is typically appropriate for self enrollment, or when a card that was issued from the CardMaker software does not yet contain any personalized data. Installations which want to specify a different initial PIN/PUK for each card that is issued from the CardMaker software - for example, installations that pre-load information to the card or card account - have the option to generate a random PIN/PUK for each card. A PIN letter is automatically generated in the Sphinx CardMaker software that can then be emailed or delivered to the end-user. Cardholders with randomly generated PIN/PUKs will not be prompted to change their PIN and PUK upon first use, but this is recommended, since the initial PIN and PUK will be the same. Not available for cards that self enroll. <u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > PIN.</i>		✓	✓
Administrator managed PUK	Organizations that issue cards from the CardMaker software can choose to keep responsibility for the PIN in the cardholder's hands, but keep the PUK accessible for the administrator, so that administrators can always unlock end-user cards. Not available for cards that self enroll. <u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > PIN.</i>		✓	✓
Require PIN/PUK change upon first use option	All Sphinx installations prompt end-user to change the initial default PIN and PUK upon first use. Installations that require an additional level of control can select the Sphinx CardMaker option which will <u>require</u> that the end-user change the initial default PIN/PUK upon first use. In this case, if the PIN/PUK is not changed, the program will not continue. <u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings</i>		✓	✓

Sphinx Feature List

	> PIN.			
PIN policy control	<p>Administrator can specify required PIN length and character type (numeric, upper case, lower case...) in Sphinx CardMaker software, and end-user must conform to these requirements.</p> <p>PIN Policy established also applies to PUK.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > PIN.</i></p>		✓	✓
PIN verification timeout	<p>Specifies the length of time that a PIN will be stored in memory. After this time, end-user will be prompted to re-enter PIN.</p> <p>Setting can be established by end-user in Sphinx Logon Manager software or Administrator in Sphinx CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Configuration > Card Settings > PIN.</i></p>	✓	✓	✓
Biometric authentication	<p>A biometric device such as a fingerprint or iris reader can be used for end-user authentication, either in combination with a card and/or PIN or by itself.</p> <p>Full biometric capabilities are completely integrated into the Sphinx software and work out-of-the-box with selected BIO-API compatible devices, including biometric enrollment and authentication.</p> <p><u>More info:</u> <i>Logon Manager User's Manual: Getting Started > Sphinx Self Enrollment > Installations with Fingerprint Readers. CardMaker Administrator's Manual: Configuration > Card Settings > PIN.</i></p>		✓	✓
Encryption	Each issued Sphinx card or Sphinx account is secured by its own unique set of TDES encryption keys. If an installation requires a specific encryption method, the modular Sphinx encryption engine can be exchanged for special customized versions.	✓	✓	✓
Secured data exchange with card	For card installations that store Sphinx data on the card, all security sensitive Sphinx data is first encrypted before being exchanged with the card.	✓	✓	✓
Card security features	Sphinx takes advantage of the card security features already offered by the powerful compatible card technologies to provide an additional layer of security. See Solution Packages at www.odsphinx.com .	✓	✓	✓
Secure web server	Sphinx CardMaker software, installed on a Windows 2000 Server or Windows 2003 Server machine, utilizes the Windows Internet Information Services challenge/response, authentication based on random number generation, and data encryption to provide secure server functionality.		✓	✓
Connection to secure server protected by SSL	<p>Installations can choose to additionally secure the data exchange between client and server via SSL.</p> <p><u>More info:</u> <i>CardMaker Administrator's Manual: Getting Started > Installation Checklist.</i></p>		✓	✓

Sphinx Feature List

Other Software Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Wide compatibility	The Sphinx software can be used out-of-the-box with all of the major card and reader technologies on the market such as contactless cards (125kHz and 13.56 MHz including Prox, Mifare, DesFire, HID iClass, Legic), contact cards (including Java, MULTOS, CardOS, Secure Memory), and MAG stripe cards. Likewise, Sphinx is compatible with PC/SC compatible desktop card readers and tokens, of which there is a wide availability on the market. See www.odsphinx.com for Compatible Products list and out-of-the-box Solution Packages.	✓	✓	✓
Built for interoperability	<p>The Sphinx software is built around open API standards to provide interoperability between platforms, card readers, cards, and third-party software solutions. Sphinx is either out-of-the-box compatible or can easily be integrated with many third-party software and hardware products. By leveraging interoperability standards, Sphinx reduces the total cost of ownership for the end customer.</p> <p>PC/SC: can be used with all PC/SC conforming smart card readers.</p> <p>ISO 7816: has built-in interfaces for a number of ISO 7816 compatible cards. ISO 7816 compatible cards that are currently not supported can easily be integrated with Sphinx.</p> <p>ISO 14443 A/B: supports ISO 14443 compatible RF cards through a number of contactless readers.</p> <p>ODBC: compatible with major database systems such as MS Access, MS SQL, Oracle, MySQL.</p> <p>LDAP: interfaces with LDAP-based directories such as Active Directory.</p> <p>COM: includes COM API for server and client-based software.</p> <p>XML: includes API based on XML-RPC function calls over IP.</p>	✓	✓	✓
Multi-language	Sphinx multi-language tool enables convenient translation and maintenance of the Sphinx program text files, including Asian languages with double-byte characters. Also enables easy branding of software for OEMs.	✓	✓	✓
Sphinx Logon Manager API for OEMs	OEMs who want to bundle Sphinx with other client applications have the option to use the built-in API to integrate further.	✓	✓	✓
Sphinx CardMaker API for third-party applications on server computer	<p>Data elements of the Sphinx CardMaker database are accessible through standard ODBC API.</p> <p>CardMaker features a flexible, built-in import function for LDAP and ODBC based data sources. This means that, for example, cardholder identification data can be imported from an HR or access control database without requiring any programming.</p> <p>All managed entries are available via an API for third party identity management and provisioning systems. Interfaces are based on ODBC, LDAP and XML-RPC standards.</p>		✓	✓



Open Domain Sphinx Solutions, Inc.
www.odsphinx.com